with each new biometric image. Thus the user identifier data may be invalidated because the UUID can change based on the modified setting or settings.

[0066] FIG. **11** is a flowchart of a method for purchasing from the online store after one or more settings for the biometric sensing device are changed. In some embodiments, the method of FIG. **11** can also be performed after the biometric sensing device and/or the electronic device being used to access the online account is rebooted. Initially, a user can be prompted for his or her password and a reason as to why the password must be entered can be provided to the user (block **1100**). As one example, the phrase "biometric sensing device settings were changed" can be displayed to the user. As another example, the phrase "biometric sensing device was rebooted" can be displayed to the user.

[0067] Next, as shown in block **1102**, the user enters his or her online password for the online store. A determination can then be made at block **1104** as to whether the entered account password matches the password stored in the user identifier data (e.g., user identifier data stored in persistent secure memory). The method ends if the password does not match the user identifier data. When the entered account password matches the user identifier data, the process passes to block **1106** an online account token can be transmitted to a secure processing device. In some embodiments, the user identifier data does not have to be remapped because the same account password is associated with user identifier data. The user is now permitted to make purchases based on a biometric image (block **1108**), and the method ends.

[0068] In some embodiments, the online account password can be deleted from the secure processing system when a user signs out of the online store or logs off the electronic device. The user identifier data, however, can still be stored in the secure processing system when the user identifier data is stored in a persistent memory.

[0069] Various embodiments have been described in detail with particular reference to certain features thereof, but it will be understood that variations and modifications can be effected within the spirit and scope of the disclosure. And even though specific embodiments have been described herein, it should be noted that the application is not limited to these embodiments. In particular, any features described with respect to one embodiment may also be used in other embodiments, where compatible. Likewise, the features of the different embodiments may be exchanged, where compatible.

1-17. (canceled)

18. A method for initiating a transaction with a website using an electronic device, comprising:

receiving at the electronic device, from a user of the electronic device, a first user input;

transmitting the first user input from the electronic device to the website;

receiving from the website and at the electronic device, an online account token;

receiving from the user, at the electronic device, a second user input;

electronically countersigning the online account token at the electronic device; and

transmitting the countersigned online account token from the electronic device to the website at least partly in response to receiving the second user input, the countersigned online account token including the online account token.

19. The method of claim **18**, further comprising:

receiving, from the website and at the electronic device, user identifier data; wherein,

the online account token is electronically countersigned with the user identifier data; and

the countersigned online account token includes the user identifier data.

20. The method of claim **18**, wherein the first user input comprises a password.

21. The method of claim **18**, wherein the second user input comprises an image of a face.

22. The method of claim **18**, wherein the second user input comprises a biometric.

23. The method of claim **22**, further comprising:

matching the received biometric to a stored reference biometric; wherein,

the countersigned online account token is transmitted from the electronic device to the website after performing the matching.

24. The method of claim **22**, further comprising:

matching the received biometric to a stored reference biometric; wherein,

the online account token is electronically countersigned after performing the matching.

25. The method of claim **24**, further comprising:

receiving, from the website and at the electronic device, user identifier data; wherein,

the online account token is electronically countersigned with the user identifier data; and

the countersigned online account token includes the user identifier data.

26. The method of claim **18**, wherein:

the website comprises an online store; and

the transaction comprises a purchase.

27. The method of claim **18**, wherein:

the online account token is received at the electronic device in response to the first user input matching user identifier data.

28. A method of making a purchase from an online store using an electronic device, comprising:

receiving an account password via a user interface displayed to a user by the electronic device;

transmitting the account password from the electronic device to the online store;

receiving from the online store, at the electronic device and in response to the account password matching user identifier data, an online account token and at least a portion of the user identifier data;

determining, by the electronic device, that a biometric sensing device of the electronic device is approved for use in completing a purchase from the online store;

capturing a biometric, using the biometric sensing device, after determining the biometric sensing device is approved for use in completing the purchase;

determining that the captured biometric matches a reference biometric;

electronically countersigning the online account token by the electronic device;

transmitting the countersigned online account token from the electronic device to the website after determining the captured biometric matches the reference biometric, the countersigned online account token including the online account token.